PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 16.10.2003

E T U O I K E U S T O D I S T U S
P R I O R I T Y D O C U M E N T

Hakija / Applicant: **Tekla Corporation, Espoo**

Patenttihakemus nro / Patent application no: **20021562**

Tekemispäivä / Filing date: **02.09.2002**

Kansainvälinen luokka / International class: **H04L**

Keksinnön nimitys / Title of invention:

"Arrangement and method for adapting mobile field device"
(Järjestely ja menetelmä liikkuvan kenttälaitteen mukauttamiseksi)

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä Patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Pirjo Kalla
Tutkimussihteeri

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

Maksu 50 €
Fee 50 EUR

Maksu perustuu kauppa- ja teollisuusministeriön antamaan asetukseen 1027/2001 Patentti- ja rekisterihallituksen maksullisista suoritteista muutoksineen.

The fee is based on the Decree with amendments of the Ministry of Trade and Industry No. 1027/2001 concerning the chargeable services of the National Board of Patents and Registration of Finland.

Osoite: Arkadiankatu 6 A, P.O.Box 1160, FIN-00101 Helsinki, FINLAND
Puhelin: 09 6939 500
Telephone: + 358 9 6939 500
Telefax: 09 6939 5328
Telefax: + 358 9 6939 5328

L1

Arrangement and Method for Adapting Mobile Field Device

Field of the Invention

This invention relates to mobile field devices, such as field computers and maintenance devices. Especially, the invention relates to applications that run in the mobile field devices. Furthermore, the invention relates to an arrangement for adapting the mobile field device to a use.

Background of the Invention

Public utilities, such as municipal electricity companies and water and sewerage utilities, (or corresponding private utilities) manage large and complex systems. The maintenance of the systems must be arranged efficiently. A traditional way, for example in a municipal electricity company, is that maintenance groups, which belong to the company's staff, know their area, and before performing tasks they go to the office of the company to get task lists and, if needed, necessary map sheets. If some unexpected tasks occur during the working day, the maintenance groups may be informed and instructed by using a radiophone, mobile phone, normal telephone, or even a fax. It may also happen that new map sheets must be picked up from the office. The control center can be informed about operations made in the field using the same ways. Alternatively, the operations can be written down on paper and transported to the office or the control center after the tasks are completed.

Some public utilities may use mobile field computers, such as PDAs (Personal Digital Assistant), for informing maintenance men in the field. However, the field computers must also be updated in the office for the use of the day, before performing the tasks. A limited amount of instruction data may be delivered to the field computer via wireless communication, but larger data amounts are impossible (or very unpractical) to transport since the capacity of the wireless communication path is limited. After the tasks are performed, the field computers may be transported to the control center for updating the system in accordance with the operations made

FIG. 1 illustrates a simple example of an energy distribution network in an area. Watercourses are marked with horizontal hatched lines and larger consumption areas with diamond hatched lines. Main roads are also illustrated on the map. The power lines 4 are marked with dashed lines,

switching stations 2 with circles, and supply transformers 3 with triangles. The generator 1 is marked with a circle with an amplitude current mark. It can be induced from the map that the distribution network comprises a great number of different elements with their attributes and parameters. For example, the energy distribution network of a city of about one million inhabitants may comprises 1,2 - 1,3 million targets (elements). The data amount, which is needed to describe a network of this size, is approximately over 100 Mbytes.

Nowadays, a trend is that public utilities externalize, for example, maintenance tasks. One company in the maintenance business may manage the maintenance of a very large area and/or of several areas, whereby the maintenance men do not any more know their areas and the networks. However, the maintenance men work the same way as before: they pick up their duties before starting to work and transport information about the operations made after the work. A problem is that the owner of the public utility (or corresponding private utility) may not desire to give all network information to the maintenance man of the external company. On the other hand, the external maintenance company may desire to use the same field devices, so it may happen that the device may contain information from several different utilities. The security of information is not as guaranteed as when the maintenance men were in the service of the utility. And as mentioned before, the huge amount of data of the systems is also a problem.

The goal of the invention is to alleviate the above-mentioned problems. This is achieved in a way described in the claims.

Summary of the Invention

According to the invention, a field mobile terminal, such as a PDA, is adapted to a use. The mobile terminal is provided with data, which is divided into several parts. Each part concerns data connected to a certain area, and the data of each part has been encrypted by using a specific encryption key or keys. The provision of data is a preliminary step for adapting the mobile terminal and it may be done in an office of a public utility or a corresponding organization. A decryption key (or keys) is location specific. The decryption keys are in a special server. When a decryption of a part (or parts) is needed, the server finds out the location of the mobile terminal. This is done by asking for the location information from a special location information

application in a communication network. The application utilizes the location information of the mobile network, which is updated in the wireless network system, such as in a GSM network. Alternatively, the location information of the mobile terminal may be delivered to the server automatically.

If the location information of the mobile terminal and the location information of one of said decryption keys matches, the decryption key is sent from the server to the mobile terminal preferably via a wireless communication path. The mobile terminal may now decrypt the data part in question for adapting the terminal for the use required.

Brief Description of the Drawings

In the following, the invention is described in more detail by means of FIGs 1 - 4 in the attached drawings where:

FIG. 1 illustrates an example of an energy distribution network in an area level,

FIG. 2 illustrates an example of dividing the data of an energy distribution network into parts, which are location specific,

FIG. 3 illustrates an arrangement according to the invention, and

FIG. 4 illustrates a flow chart that shows an example of the inventive method.

Detailed Description of the Invention

Suitable data and software must be set up in the mobile field terminal, which can, for example, be a field computer, mobile maintenance device, a PDA, or a mobile phone, to adapt it for use. Lets examine an example of a power distribution network illustrated in FIG. 1. If the network information is utilized in an efficient and inventive way according to the invention, it must be divided into several parts. Preferably, the division may be based on geographical areas, such as rectangles in a map or other geographically logical areas (valleys, mountains etc.), but it may also be based on the structure of the distribution network - the area of a distribution substation may be a part. However, each part has always some location in a geographical map.

FIG. 2 shows an example of the division of the power distribution network based on the rectangles 21. For example, rectangle B11 contains the information from one switching station 22, two supply transformers 23,

24, and the distribution lines 4 in the area of the rectangle. When maintenance men are in the area of B11 for performing their tasks, they do not usually need information from the other parts of the network - just the information from part B11. The maintenance men carry the mobile field terminal, which contains all information from the distribution network, but only the information of part B11 is accessible. The maintenance men can do their tasks in the area of B11, and receive new tasks and send performed tasks to the control center via a wireless communication path. When they move to another area, for example, to part A12, the decryption key of the new area is accessible from the server, but the key of the old area B11 is no longer accessible. In this way, the mobile terminal is always adapted to the use in question.

The divided (and encrypted) information of the distribution network is downloaded to the mobile terminal from a server, which contains the information of the distribution network. Naturally, the server and the mobile terminal are connected to each other during the download. The connection can be a cable connection, a connection through a fixed network, or even a connection through a wireless network. However, if the connection is through a wireless network, the time required for the download is very long depending on the low transmission capacity of the wireless network and the huge data amount of the network. The wireless solution may be reasonable at nights. It may be also needed to download special software for using and utilizing the network information.

Each part of the network information has been encrypted by a part specific key (or keys if the encryption is based on several keys). Also the special software may be divided, according to the division of the information, into parts, and encrypted as well. When maintenance of a certain network element in a certain area (part) requires special software, it is accessible at the same time as the information needed. The encryption may be based on key pairs and enough long bit codes etc.

The encrypted information parts (and the pieces of software) make it possible that only the part or parts needed are accessible to the maintenance men. Decryption is needed for accessing the information needed. Since the encrypted information is connected to a certain area, i.e. location, the decryption key or keys are location specific. The encryption mechanism may be utilized as key pairs. (Other ways are possible as well.) I.e. the encrypting key and decrypting key of a certain part perform as a key pair. The

decryption keys are not in the mobile terminal, but they are in a special server from which they have to be transported to the mobile terminal. In order to deliver the decryption key or keys needed, the location of the mobile terminal must be determined. When the location of the mobile terminal and the location information of the decryption key matches, the decryption key is transported to the mobile terminal wirelessly. In other words, the decryption key or keys, corresponding to the location of the mobile terminal, are transported to the terminal for decrypting the information (and the piece of software) of the part of that location. When the terminal moves away from the area the decryption key in the server may again become inaccessible (The key is not delivered to the mobile terminal.) based on the location information that the mobile terminal gets from the network system (the network system has to known the location of the mobile terminal).

FIG. 3 shows an example of an inventive arrangement. The server **31**, wherein the decryption keys **311** lie, preferably finds out the location of the mobile terminal **32** from a location service **34** via a network **35**. The location service utilizes the location information system **33** of the network to which the mobile terminal is connected, normally wirelessly. A very common system is the use of the location information system of the mobile network, such as GSM or UMTS. So the location service gets location information from the location information system.

The server asks for the location information of the mobile terminal from the location service. As a response to this enquiry, the location service transports the location information. Alternatively the server may ask for the location information from the mobile terminal itself, but this is not a recommended way, since it is not so secure. (The mobile terminal should get its location information from the location information system **33** since the location information from the mobile terminal may be a fake.) It is also possible that the location service (or the mobile terminal) automatically, without any request, transports location information to the server, so that the server always knows the locations of the mobile terminals that are under its service.

A preferable way is that the mobile terminal asks for a decryption key (or keys) from the server, which, as a response, finds the location of the mobile terminal, searches the right decryption key, and transports it to the mobile terminal. Naturally, in the case of an automatic delivery, no request is needed to be sent from the mobile terminal.

The mobile terminal comprises means **321** for decrypting the part/s needed using the decryption key or keys. Further, the mobile terminal comprises means **322** for adapting the mobile terminal for the use. This means that not only the decrypted information of the part is saved in the mobile terminal, but also the software needed, and maybe related functions, are installed. Furthermore, the mobile terminal may comprise means for requesting the decryption key or keys from the server.

The server comprises the decryption keys **311**, as mentioned before, and means **312** for providing the mobile terminal with data, which is divided into several parts, each part concerning data connected to a certain area, and said data of each part encrypted by a location specific key. The providing means are connected to the mobile terminal for the duration of the provision of data. Naturally the providing means may be in another element than the server. Further, the server comprises means **313** for finding out the location of the mobile terminal, means **314** for comparing the location information of the mobile terminal and the location information of said decryption keys, and selecting that decryption key (or keys) whose location information and the location information of the mobile terminal match, and means **315** for sending the selected decryption key (or keys) from the server to the mobile terminal as a response to the actions of the comparing and selecting means **314**.

Further, the means for finding out location information may comprise means for requesting the location information of the mobile terminal from a location service that is in connection with the server through a communication network, or from the mobile terminal, and means for receiving the requested information.

FIG. **4** shows an example of the inventive method in a flow chart form. First the mobile terminal is provided **51** with data, which is divided into several parts, each part concerning data connected to a certain area, and said data of each part encrypted by a specific key or keys. When the mobile terminal has been provided with the information (and software) according to the invention, the next step is taken for adapting the terminal for the use, preferably for the current use. The server finds out **52** the location of the mobile terminal. In this step, the server may ask for the location information preferably from the location service, or the location information may be transported to the server automatically. As mentioned, the server comprises the

location specific decryption keys. If the location information of the mobile terminal and the location information of one of said decryption keys matches, said decryption key or keys are sent **53** from the server to the mobile terminal. In the mobile terminal, the part to which said decryption key matches is encrypted **54**. And as mentioned, the adaptation of the mobile terminal may contain other tasks along with the decryption function.

It should be noted that location information need not necessarily be the only criteria to check the validity to transport the decryption key from the server to the mobile terminal. Along with the location information, the decryption key may also be associated with the identification of the mobile terminal and/or time information. In this way, it is possible to classify users in more detail and to increase the security of the data. For example, if the mobile terminal belongs to a certain subcontractor, it may be desirable to give him only a certain part of the information. It may also desired that the information of the parts is accessible only during a certain period, then time information is needed for the decryption function: the information may be decrypted in day time, but not in evenings or at nights for example. Naturally, combinations of different criteria may be used.

The decryption function may not be restricted to one part of the information, but it may be useful that several parts are also decrypted at the same time. For example, if the maintenance men are in the area of B11 in FIG. **2**, and the server has this location information, the maintenance men may be allowed to get an access to the parallel parts of B11 as well, i.e. to parts A11, C11, A12, B12, and C12. This is convenient to arrange by transporting the decryption keys of the parallel parts with the decryption key of B11.

The invention makes it possible to use external maintenance companies in a safe way. The security of the information of a public utility (or private utility or another company) is high, since the information itself is not transported over a wireless communication path, but only the decryption key or keys of the information allowed to be used, is transported. A subcontractor has access only to the information needed for his duties. Anyway, wireless transmission of huge data amounts requires an unacceptable long period and is expensive as well. So, the invention saves the transmission capacity of the communication network as well and is an economical solution. It is also relatively safe to ask for location information from a special location service. The

alternative is to ask the location information from the mobile terminal, but then the security level is lower. So, the information is very quickly in the use of the subcontractor in a secure way.

Decryption keys allow various different solutions. A number of keys may concern the same area. One key decrypts a small subarea, another key a larger area, etc. Or one key decrypts certain information in the area and another key other information. The decryption keys of several areas may be delivered at the same time, or several keys are needed for decrypting one area.

One application of the invention may be that when using the identification information of the mobile terminal along with the location information, certain sensitive information in the part may be decrypted separately from the main decryption of the part of the information. The sensitive information is allowed only to the certain terminal or terminals. Other terminals can decrypt the information of the part, but without the sensitive material. As noted, the invention is for professional use, concerning maintenance actions of an organization, such as different public utilities. It is evident that the invention can be used in other ways than described in this text, so it can be used in many different solutions, in the scope of the inventive idea.

L 2

Claims

1. A method for adapting a mobile terminal to a use, characterized in that the method comprises the preliminary step of providing the mobile terminal with data, which is divided into several parts, each part concerning data connected to a certain area, and said data of each part encrypted by a specific key or keys,

the provided data being in the mobile terminal the method comprising the steps of:

- finding out a location of the mobile terminal by the server, the server comprising location specific decryption keys,
- if the location information of the mobile terminal and the location information of one of said decryption keys match, sending said decryption key or keys from the server to the mobile terminal, and
- decrypting the part to which said decryption key matches for adapting the mobile terminal for the use.

2. A method according to claim 1, characterized in that prior to sending the decryption key or keys, the mobile terminal requests the decryption key or keys from the server.

3. A method according to claim 1 or 2, characterized in that the step of finding out the location of the mobile terminal comprises the step of requesting the location information from a location service in the network and as a response to said enquiry the location service transports the requested location information to the server.

4. A method according to claim 1 or 2, characterized in that the step of finding out the location of the mobile terminal comprises the step of transporting the location information from a location service in the network to the server.

5. A method according to claim 1 or 2, characterized in that the step of finding out the location of the mobile terminal comprises the step of requesting the location information from the mobile terminal and as a response to said enquiry the mobile terminal transports the requested location information to the server.

6. A method according to claim 1, characterized in that the step of finding out the location of the mobile terminal comprises the step of requesting the location information from a location service in the network

or from a mobile terminal and as a response to said enquiry the location information is transported to the server, which location information the server utilizes when automatically matching and sending said decryption keys.

7. A method according to claim 3, characterized in that the location service utilizes the location information of the mobile terminal, which is within the knowledge of the network.

8. A method according to claim 5, characterized in that the mobile terminal utilizes the location information of the mobile terminal, which is within the knowledge of the network.

9. A method according to any of claims 1 - 8, characterized in that along with the location information, identification information of the mobile terminal is used for matching the decryption key or keys.

10. A method according to any of claims 1 -8, characterized in that along with the location information, time information is used for matching the decryption key or keys.

11. A method according to any of claims 1 - 8, characterized in that along with the location information, identification information of the mobile terminal and time information are used for matching the decryption key or keys.

12. A method according to any of claims 1 - 11, characterized in that decryption keys for several parts are transported to the mobile terminal for adapting the mobile terminal.

13. A method according to any of claims 1 - 12, characterized in that the adaptation is made for a current use.

14. An arrangement for adapting a mobile terminal to a use, characterized in that the arrangement comprises:

- a first means for providing the mobile terminal with data, which is divided into several parts, each part concerning data connected to a certain area, and said data of each part encrypted by a location specific key, which providing means are connected to the mobile terminal for the duration of the provision, location specific decryption keys in a server,
- a second means for finding out a location of the mobile terminal in the server,
- a third means in the server for comparing the location information of the mobile terminal and the location information of said

decryption keys, and selecting that decryption key whose location information and the location information of the mobile terminal match,

- a fourth means in the server for sending the selected decryption key from the server to the mobile terminal through an available network as a response of the third means
- a fifth means in the mobile terminal for decrypting the part using the decryption key.

15. An arrangement according to claim 14, characterized in that the mobile terminal comprises a sixth means for requesting the decryption key or keys from the server.

16. An arrangement according to claim 15, characterized in that the mobile terminal comprises a seventh means for adapting the mobile terminal for the use.

17. An arrangement according to claim 14 or 16, characterized in that the second means comprises means for requesting the location information of the mobile terminal from a location service that is in connection with the server through a communication network, or from the mobile terminal, and means for receiving the requested information.

18. An arrangement according to claim 14 or 17, characterized in that the decryption keys are further associated with time information and/or identification information of mobile phones, which is used along with the location information when comparing these pieces of information and selecting the decryption key.

19. An arrangement according to any of claims 14 - 18, characterized in that the mobile terminal is a field computer, PDA or mobile phone.

20. An arrangement according to any of claims 17, characterized in that the location service utilizes location information from a mobile phone network.

21. An arrangement according to any of claims 14 - 20, characterized in that as response to the third means, the fourth means sends decryption keys for several parts for adapting the mobile terminal.

L3

1

(57) Abstract

The invention relates to an arrangement for adapting a mobile field device to a use. According to the invention, a field mobile terminal, such as a PDA, is adapted to a use. The mobile terminal is provided with data, which is divided into several parts. Each part concerns encrypted data connected to a certain area. Decryption keys are in a special server. When the decryption of the part is needed, the server finds out the location of the mobile terminal. If the location information of the mobile terminal and the location information of one of said decryption keys match, the decryption key is sent from the server to the mobile terminal. The mobile terminal may now decrypt the data part in question for adapting the terminal for the use.

(Fig. 3)

L4

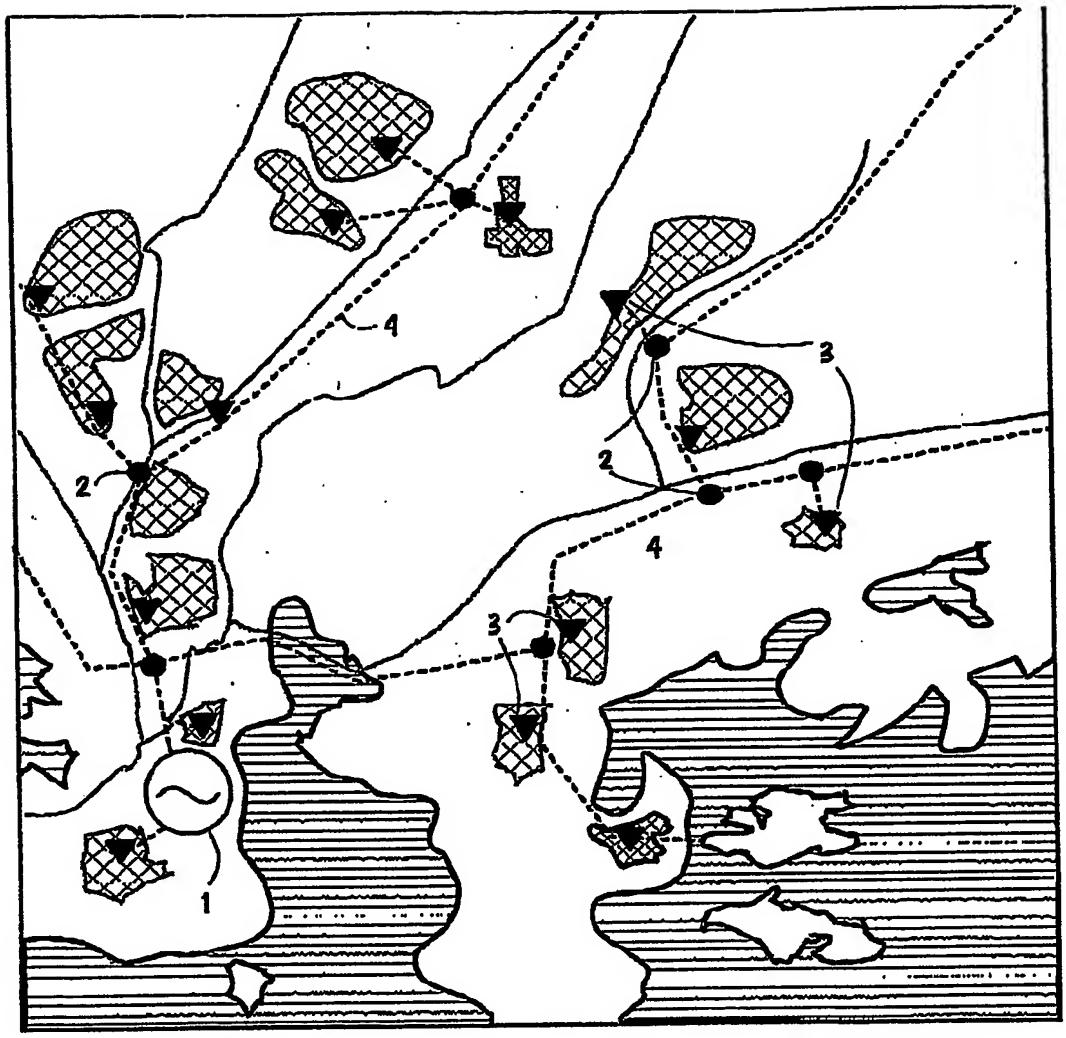

FIG.1

LY

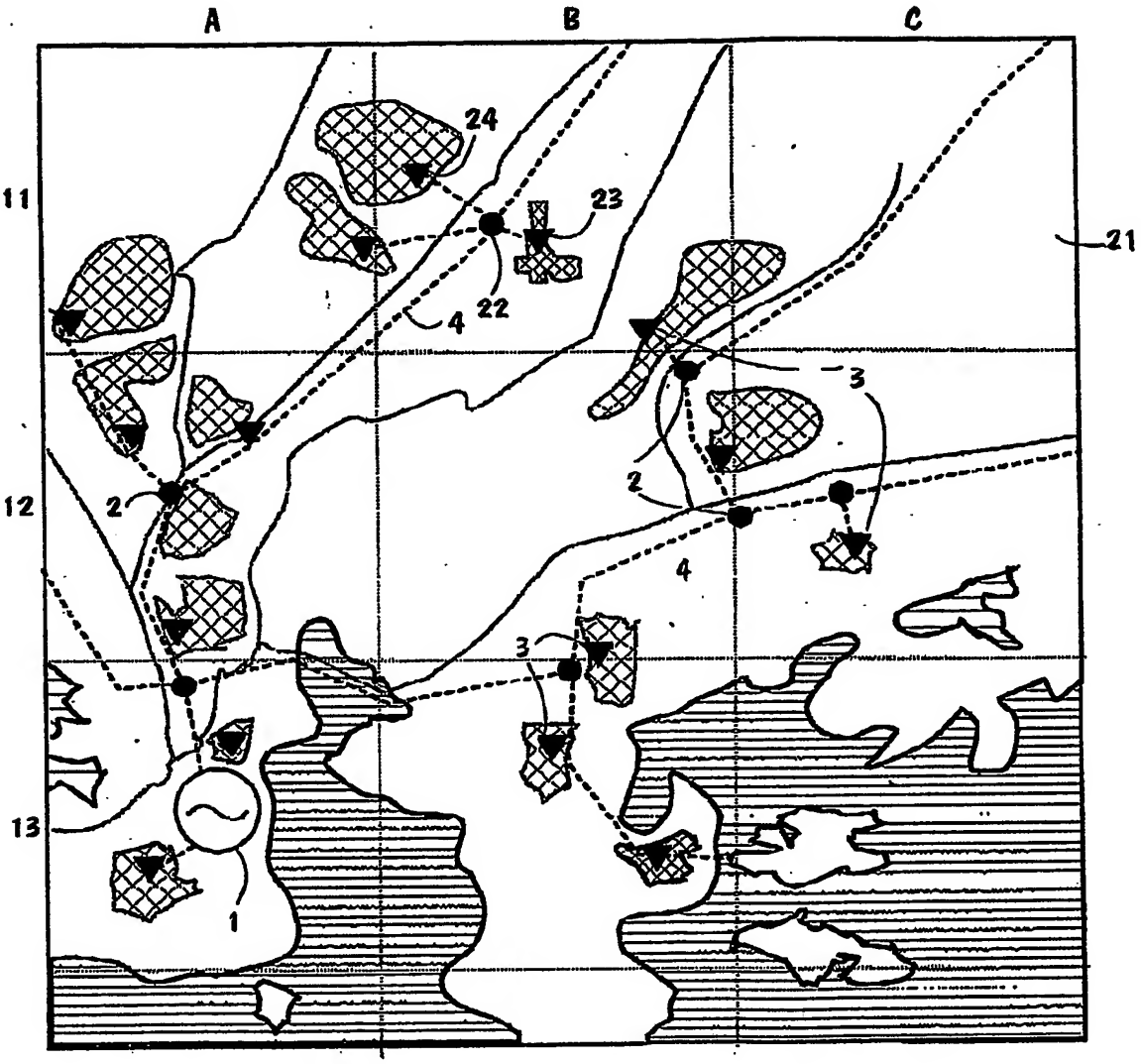

FIG.2

L4

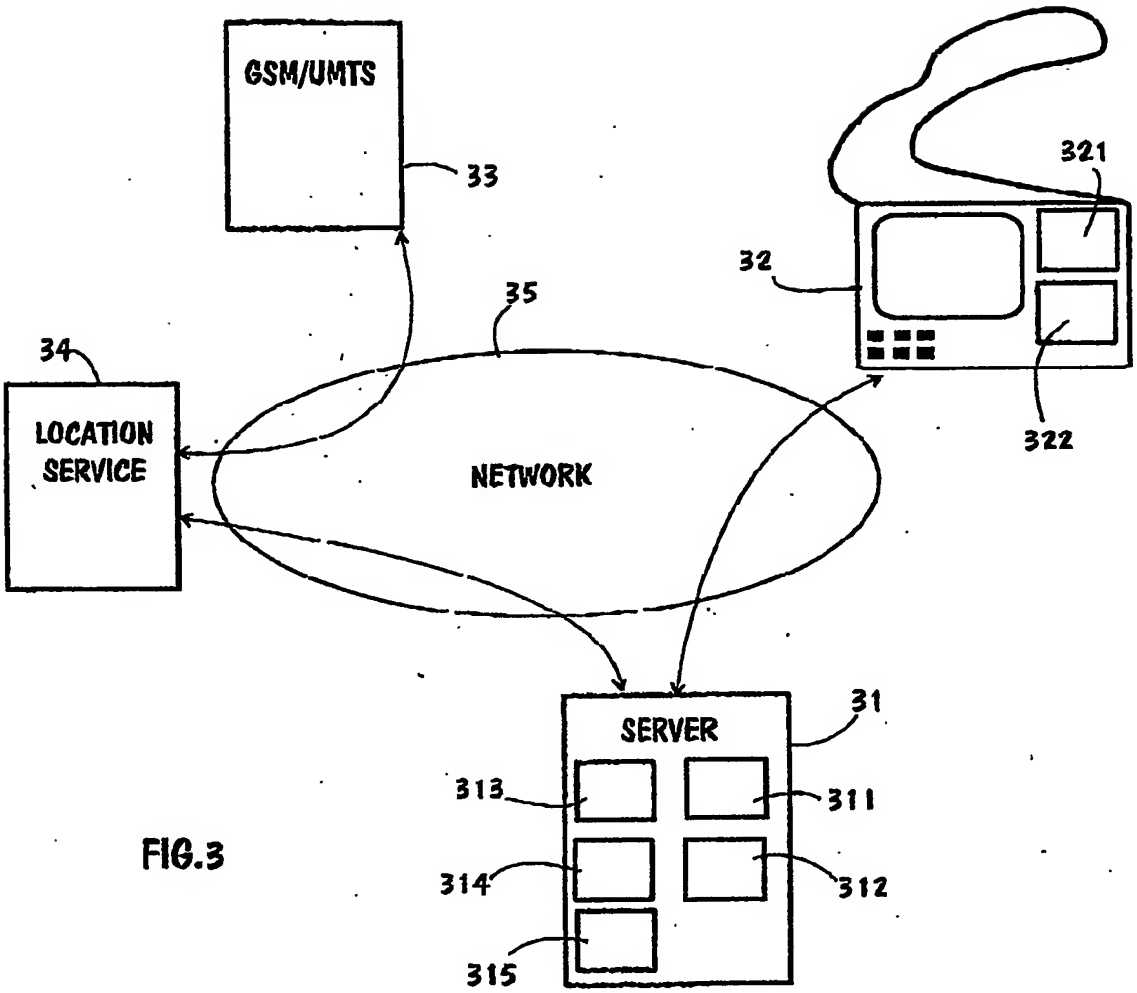
GSM/UMTS
33
321
32
35
34
LOCATION SERVICE
NETWORK
322
SERVER
31
313
311
314
312
315

FIG.3

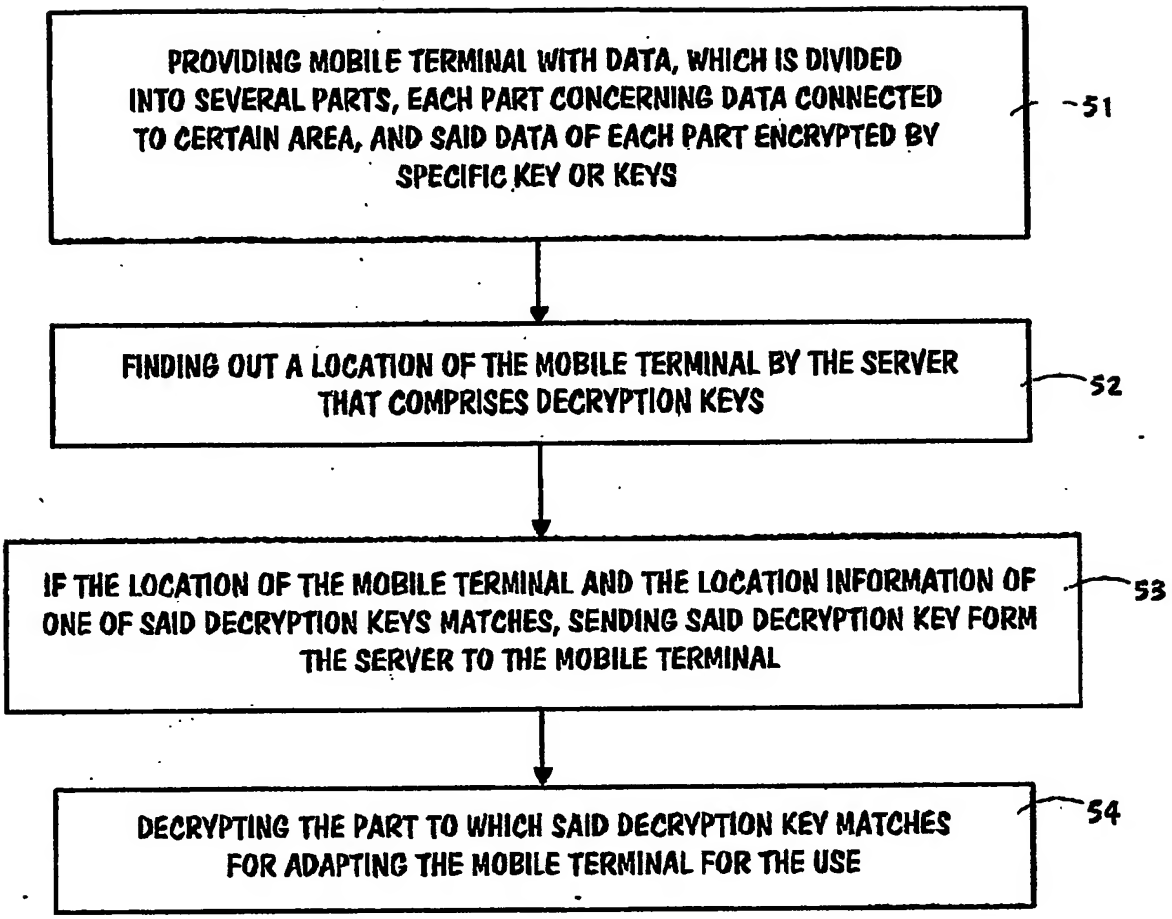
PROVIDING MOBILE TERMINAL WITH DATA, WHICH IS DIVIDED INTO SEVERAL PARTS, EACH PART CONCERNING DATA CONNECTED TO CERTAIN AREA, AND SAID DATA OF EACH PART ENCRYPTED BY SPECIFIC KEY OR KEYS
51
FINDING OUT A LOCATION OF THE MOBILE TERMINAL BY THE SERVER THAT COMPRISES DECRYPTION KEYS
52
IF THE LOCATION OF THE MOBILE TERMINAL AND THE LOCATION INFORMATION OF ONE OF SAID DECRYPTION KEYS MATCHES, SENDING SAID DECRYPTION KEY FORM THE SERVER TO THE MOBILE TERMINAL
53
DECRYPTING THE PART TO WHICH SAID DECRYPTION KEY MATCHES FOR ADAPTING THE MOBILE TERMINAL FOR THE USE
54

FIG.5